1988-03

A methodology for designing local area networks for the Air Force

Cleveland, Jannine Lee Ann

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A METHODOLOGY FOR DESIGNING
LOCAL AREA NETWORKS FOR THE AIR FORCE

by

Jannine Lee Ann Cleveland

March 1988

Thesis Advisor: Neil Rowe

UNCLASSIFIED

ECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
b. DECLASSIFICATION/DOWNGRADING SCHEDULE -	
. PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)

a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) Code 39	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
c. ADDRESS (City, State, and ZIP Code)		10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO	WORK UNIT ACCESSION NO.

. TITLE (Include Security Classification)
A METHODOLOGY FOR DESIGNING LOCAL AREA NETWORKS FOR THE AIR FORCE

. PERSONAL AUTHOR(S)
Cleveland, Jannine L. A.

a. TYPE OF REPORT Master's Thesis	13b TIME COVERED FROM ______ TO ______	14. DATE OF REPORT (Year, Month, Day) 1988 March	15 PAGE COUNT 86

. SUPPLEMENTARY NOTATION

COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Local area networks, LAN, network interface units, network management, baseband and broadband coaxial cable, token passing, carrier sense media access/collision detection

. ABSTRACT (Continue on reverse if necessary and identify by block number)

This thesis effort examines applying local area network (LAN) technology to the Air Force. Long haul nets such as the Automatic Digital Network (AUTODIN) and Defense Data Network (DDN) are vital elements of command and control (C2) for the Air Force, but this functionality has not yet been extended to cover base-level C2 requirements. The principle elements of this study concern the need for LANs on Air Force bases, the best local area network design for Air Force bases, and a local area network implementation strategy.

LANs have the additional advantage of being able to provide information sharing between microcomputers that use different operating systems. Three interconnection scenarios are described and potential solutions for each one are presented, with the autor's recommendation for the best solution in each case. These solutions build the case for Air Force local area network standards: a broadband backbone connecting a variety of networks designed to support a variety of users.

. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
a. NAME OF RESPONSIBLE INDIVIDUAL Neil Rowe	22b TELEPHONE (Include Area Code) (408) 646-2462	22c. OFFICE SYMBOL Code 52RP

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

U.S. Government Printing Office: 1986—606-243

UNCLASSIFIED

Approved for public release; distribution is unlimited.

A Methodology for Designing Local Area Networks for the Air Force

by

Jannine Lee Ann Cleveland
Captain, United States Air Force
B.S., State University of New York, 1977

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
March 1988

ABSTRACT

This thesis effort examines applying local area network (LAN) technology to the Air Force. Long haul nets such as the Automatic Digital Network (AUTODIN) and Defense Data Network (DDN) are vital elements of command and control (C2) for the Air Force, but this functionality has not yet been extended to cover base level C2 requirements. The principal elements of this study concern the need for LANs on Air Force bases, the best local area network design for Air Force bases, and a local area network implementation strategy.

LANs have the additional advantage of being able to provide information sharing between microcomputers that use different operating systems. Three interconnection scenarios are described and potential solutions for each one are presented, with the author's recommendation for the best solution in each case. These solutions build the case for Air Force local area network standards: a broadband backbone connecting a variety of networks designed to support a variety of users.

TABLE OF CONTENTS

LIST OF TABLES ---- 6

LIST OF FIGURES ---- 6

I. INTRODUCTION ---- 7

A. GENERAL ---- 7

B. OBJECT OF RESEARCH ---- 9

C. RESEARCH QUESTIONS ---- 9

D. SCOPE, LIMITATIONS, ASSUMPTIONS ---- 10

E. METHODOLOGY ---- 12

F. SUMMARY ---- 12

II. LOCAL AREA NETWORK OVERVIEW ---- 13

A. WHAT IS A LAN? ---- 13

B. TYPES OF LANS (TOPOLOGY) ---- 14

C. COMPONENTS OF A LAN ---- 18

D. LAN MEDIA ACCESS METHODS ---- 25

E. THE ISO OSI MODEL ---- 26

F. SUMMARY ---- 29

III. AIR FORCE OPERATIONAL REQUIREMENTS ---- 30

A. WHAT DOES A LAN REPLACE? ---- 30

B. WHAT ADDITIONAL SERVICES WILL A LAN SUPPORT? - 31

C. WHAT A LAN ISN'T ---- 32

D. REQUIREMENTS ---- 33

E. SUMMARY ---- 35

IV. PROBLEMS IN IMPLEMENTING A STANDARD AIR FORCE LAN 36

A. CONCEPT ---- 36

B. COST OF CONNECTION ---------------------------- 36

C. FUNDING -- 37

D. ADP VERSUS COMMUNICATIONS -------------------- 39

E. AVAILABILITY ---------------------------------- 39

F. TYPICAL INTERCONNECTION SCENARIOS ------------ 40

G. SUMMARY -- 53

V. RECOMMENDATIONS ------------------------------------ 54

A. INTRODUCTION ---------------------------------- 54

B. DESIGN -- 55

C. IMPLEMENTATION -------------------------------- 57

D. SUMMARY -- 58

APPENDIX A: DEFINITIONS AND ABBREVIATIONS -------------- 59

APPENDIX B: HQ USAF/SIT 012200Z SEP 84 MESSAGE --------- 62

APPENDIX C: SUMMARY OF AFLANSPO USER REQUIREMENTS SURVEY, AS BRIEFED MARCH 1985 ----------- 75

APPENDIX D: SAMPLE QUESTIONNAIRES FOR INTERCONNECTION SCENARIOS ------------------------------- 78

LIST OF REFERENCES ---------------------------------- 83

BIBLIOGRAPHY -- 84

INITIAL DISTRIBUTION LIST ---------------------------- 85

LIST OF TABLES

1. LAN TOPOLOGIES -- 16

2. TRANSMISSION MEDIA ------------------------------------ 19

LIST OF FIGURES

1. LAN TOPOLOGIES -- 15

2. ISO OSI REFERENCE MODEL ------------------------------ 27

3. TOKEN PASSING RING FOR A SMALL OFFICE --------------- 43

4. INTRABUILDING BROADBAND TREE FOR A LARGE
ORGANIZATION ------------------------------------ 47

5. INTERBUILDING MESH FOR A LARGE, DISPERSED
ORGANIZATION ------------------------------------ 52

6. POTENTIAL LAN SOLUTION FOR AN AIR FORCE
INSTALLATION ------------------------------------ 56

I. INTRODUCTION

A. GENERAL

A local area network (LAN) provides the transmission media and intelligence to connect a variety of user devices. A LAN uses protocols to send and receive information between a variety of user devices. The protocols provide the intelligence through a structured way of handling the data and the means for connection (i.e. wire) is the transmission medium. A user device can be anything from a mainframe computer to a dot matrix printer.

The recent merger of the communications (30XX) and data automation (51XX) career fields into the information systems (49XX) Air Force specialty code aptly demonstrates the blurring of the lines between automatic data processing (ADP) and communications-electronics (C-E). The rapid development and use of local area networks in both business and the military further reduces the distinction between the two disciplines.

The increased use of personal computers, work stations, and word processing equipment in the Air Force office environment coupled with long experience with the convenience of the Defense Communications Agency's long haul networks for electronic transfer of information has led to user dissatisfaction with "air-gap" connectivity in the local environment.

Uncontrolled and uncoordinated automation of functions has led to a proliferation of terminals hardwired to a single mainframe computer. If systems need to share data, the data is often printed out from one terminal and manually entered into another system using the other system's terminal. This "air-gap" technology defeats the purpose of automation--to increase productivity. The maintenance control center at Spangdahlem Air Base is an example of automation gone wild. [Ref. 1] Several inventory functions (i.e. weapons, fuel, transportation, flight line, supply) were automated and a terminal for each placed in the maintenance control center. The proliferation of computers (and therefore databases) is the result of two requirements: having the mainframe near the work area and providing redundancy. If information available in the supply database is needed to update a record in the fuel database, it is printed out or sent to the screen of the supply system terminal where it is read and retyped on the fuel system terminal. Because of this, the databases do not always provide accurate information. If the database is shared, then all involved organizations can make decisions based on current, accurate information.

B. OBJECT OF RESEARCH

The purpose of this research is to outline a strategy for an overall, multi-purpose local area network design suitable for a variety of Air Force applications. Once the technology is implemented, support for automation of functions such as inventory control will be part of the overall information systems plan for a particular location. Several LAN designs will be discussed to show how local network technology can solve the "air-gap" problem. The primary applications required are file transfer, database sharing, and electronic mail.

C. RESEARCH QUESTIONS

The primary question considered in this research is, "Can a single LAN design satisfy Air Force users?" The design variables are cost, size of network (distance and number of users), and reliability. This focus emphasizes the unique aspects of Air Force base level operations. A corporate headquarters or industrial complex might be as large as an Air Force base, but the corporation has centralized control over the devices to be connected by a local area network through total control of the budget and acquisition process, whereas Department of Defense agencies have to justify annual budgets to Congress, deal with changing acquisition regulations, and do not have consolidated control of acquisitions, even at the base level.

There is also intense competition between Air Force major commands (MAJCOMs) for available funds.

D. SCOPE, LIMITATIONS, AND ASSUMPTIONS

This thesis is motivated by the three year search for standards for an Air Force LAN. The scope of this thesis is limited to fixed base information transfer requirements, and does not include mobile tactical systems. However, most mobile systems could probably connect through a Defense Data Network (DDN) terminal access controller (TAC).

The primary limitation of this thesis is that security considerations will not be addressed. Many users have classified information transfer requirements which must be addressed for local networks. An additional security risk is encountered when previously separate and unclassified databases become connected to the same network providing correlations that in aggregate become classified. The security issue may be the subject of another thesis.

Another limitation is the omission of a discussion on private automatic branch exchanges (PABXs) serving as LANs. Some information transfer requirements can be totally satisfied by the data transfer ability of the latest electronic switching systems. The sole use of PABXs was not included in order to limit the scope of this thesis.

The primary assumptions of this thesis center around the Air Staff mandated protocols for data communications and the

International Standards Organization (ISO) Open System Interconnection (OSI) model. It assumes the protocols specified in HQ USAF/SIT 012200Z Sep 84 message, "Policy and Guidelines on Data Communications Protocols," will be used. (See Appendix B.) This message was sent out for two reasons: to provide interim local area network standards until the Unified Local Area Network Architecture (ULANA) was ready, and to slow down the acquisition of non-standard local networks within the Air Force. At the time the message was sent, the demand for local area networks within the Air Force was so high, it appeared that many users would have some kind of network before the Air Force had any standards. Because of the importance Air Staff placed on LAN standards, this message mandated the use of MIL-STD protocols 1771 through 1789 in an effort to provide standards for near term and ongoing acquisitions.

Resistance to the implementation of the mandated Transmission Control Protocol (TCP, MIL-STD-1778) and Internet Protocol (IP, MIL-STD-1777) at the network interface unit (NIU), instead of at the network boundary, has been high for two reasons: the increased cost of NIUs and the fact that TCP/IP are not international standards. Modifications to the ISO OSI model have been proposed, but will not be considered here. Examination of either assumption could be the basis of further research.

E. METHODOLOGY

The basic methodology used in this thesis is one of evaluation. In particular, the available local area network topologies, transmission media, media access methods, and their applicability to Air Force bases, or installations, will be examined.

F. SUMMARY

Although local area network technology is here today, the Air Force has not yet approved a set of comprehensive standards. The lack of standards in local network acquisition leads to noninteroperability in the operational environment. The Air Force is waiting for development of industry standards that support its security and rapid reconfiguration requirements.

The security aspect has already been discussed and the reconfiguration problem is addressed in the network management portion of this thesis. If industry standards are used, then the Air Force (and Department of Defense) will not have to fund the research and development of the components that support those standards. The increased use of requirements contracts for industry (not Department of Defense) standard ADP and communications products will support use of an industry standard local area network.

II. LOCAL AREA NETWORK OVERVIEW

A. WHAT IS A LAN?

According to the Unified Local Area Network Architecture (ULANA) A-level specification (10 Oct 85),

> The ULANA program will provide the standard hardware and software products necessary for intra-base information flow among end-user devices, dedicated systems, shared systems, and gateways to other information transfer systems. [Ref. 2]

This specification was written for the Air Force Local Area Network Systems Program Office (AFLANSPO) at the Air Force System Command (AFSC) Electronic Systems Division (ESD). The AFLANSPO was chartered to develop standards for an Air Force local area network.

A definition from outside the Department of Defense follows:

> A local area network is a communications facility that covers a limited topology and interconnects in an effective manner different types of servers and work-stations, more particularly personal and professional computers. In width it varies from 100m to nearly 10km depending on the architecture. [Ref. 3]

Commonality in the above definitions is found in the terms "information flow" and "communications." Another point of agreement is found in the phrases "hardware and software products necessary" and "interconnects in an effective manner." Therefore, a LAN should provide the intelligence to connect heterogeneous devices; it is a smart transmission path. The ability to connect and support communications between heterogeneous devices is crucial to the Air Force. Until the recent standardization of Department of Defense computer acquisition, there was no way to control the types of computers being purchased within the Air Force (or the Department of Defense as a whole); there are now diverse types of endpoint objects (EPOs) in the Air Force inventory. Many of these EPOs require connectivity to other EPOs for data and resource sharing. The services and types of connectivity supported will be discussed in section III.

B. TYPES OF LANS (TOPOLOGY)

The basic topological types of local nets are star, ring, bus, tree, and mesh. (See Figure 1, Table 1.) For LANs, the terms topology and architecture are interchangeable.

The star LAN has a central processor connected point-to-point with every endpoint object on the network. This type of network can be economically installed in buildings that have available data grade twisted pair telephone wire. Depending on the type of central processor, the network may be able to stay on-line when new users are added. However, the central processor can be a single point of failure.

The devices of the ring, or loop, local network are connected in a closed circle along the transmission medium.

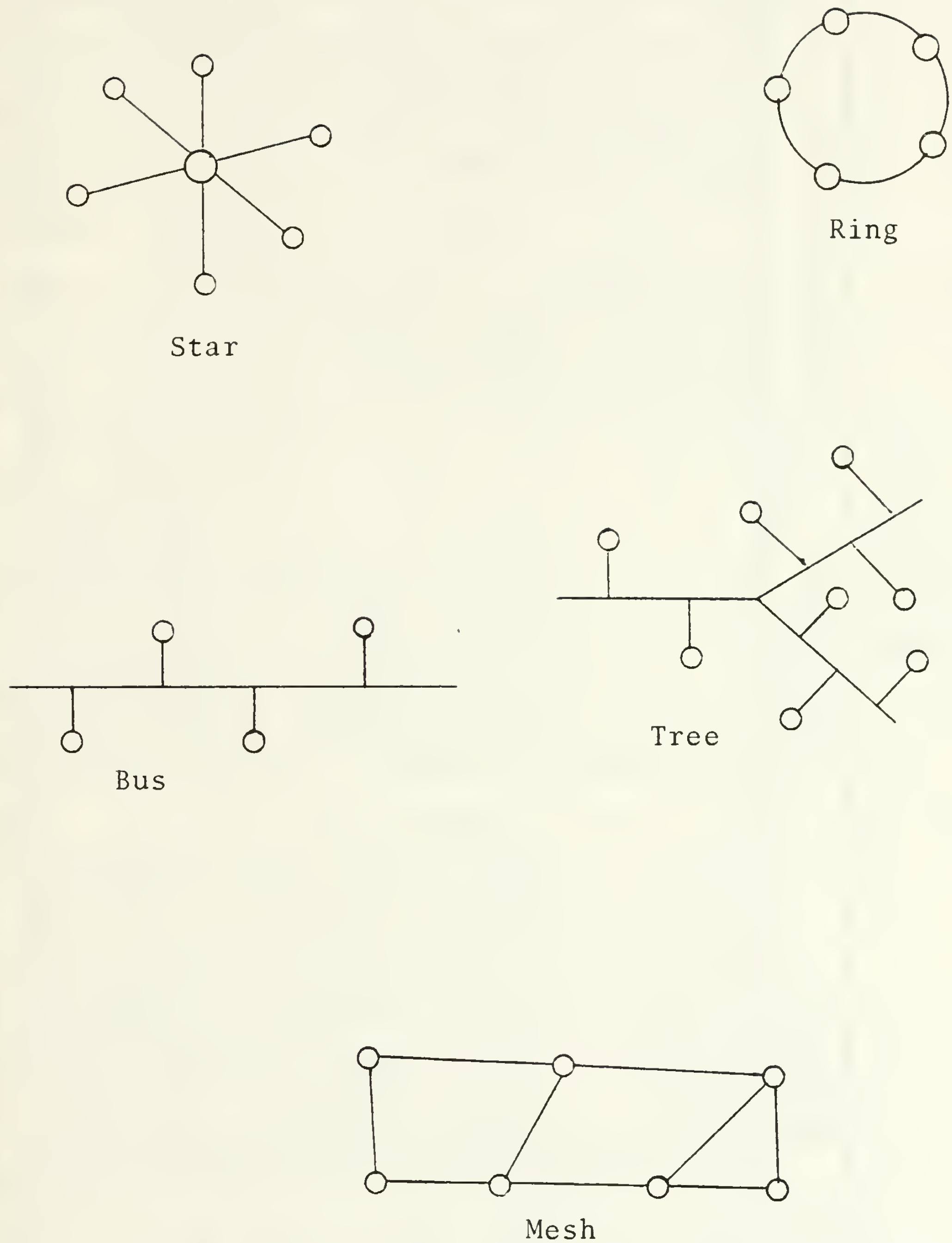

Figure 1 LAN Topologies

TABLE 1

LAN TOPOLOGIES

	PRIMARY APPLICATION	MAX NUMBER OF NODES	TRANSMISSION RATES
STAR	connect terminals to a central computer	64	depends on media; generally low since main advantage is use of twisted pair; some are very high speed (>10Mbps) using optical fiber to connect high speed devices (i.e. mainframes)
RING	connects co-equal nodes for resource and process sharing	50; limited by lack of network management	depends on txn medium, no. of nodes; rings must use token passing; 10Mbps max
BUS	prioritizing and connecting unequal nodes for resource and process sharing	depends on media and length, about 100 per .5km	depends on transmission media, no. of nodes, and size of LAN; 1-10Mbps
TREE	extension of bus	same as bus	same as bus
MESH	same as bus, and provides at least two paths between any two nodes for redundancy	in theory same as bus; in practice slightly less due to more complex net management	same as bus

The ring is easy for the user to implement in a small office environment. Use of parallel (or dual) rings for connection on a larger system allows for fault detection and allows new users to be added without disrupting service to the other users. For single ring nets, failure of a single device can result in total failure of the network and the network must be brought down to add a new user.

The bus network consists of devices joined to a linear strip of transmission medium. The bus can support single or multiple channel operations. This configuration is more flexible and less vulnerable than the star or ring. Failure of a single device will not cause failure of the entire network and the network does not have to be reconfigured when new devices are added. If extra turnaround frequency translation points (headends) are provided, a break in the transmission path will segment, but not bring down, the network. However, a single break in the transmission path may cause network failure if certain design precautions are not taken (i.e., use of redundant headends).

The tree is a variation of the bus architecture where the main transmission path is split into branches. There is only one route between any two devices. This topology avoids the problem of a single break in the path causing network failure. However, a break would isolate portions of the network.

The mesh architecture provides multiple routes between any two endpoint objects. It is therefore a highly reliable and flexible topology. The drawback is the complex routing and flow control required. Although widely used in long-haul communications, the cost and complexity can be prohibitive in most local network environments.

C. COMPONENTS OF A LAN

There are three major components of a local area network: the transmission medium, the interface units, and a network management system.

1. Transmission Medium

The transmission medium is the physical matter the communications signals from one device must flow through to get to another device. The main categories for LAN transmission media are twisted pair copper wire, coaxial cable, and optical fiber. (See Table 2.).

Twisted pair, or multiple pair twisted copper wire, is the simplest and least expensive transmission medium (cable). Most telephone systems use this type of cable. Twisted pair can be used with any topology, but it has the following drawbacks: it is highly susceptible to external noise interference, data rates decrease as the distance increases, and the error rate increases as the data rate increases. The vulnerability to external noise is largely from the inexpensive wrapping on the wire. The maximum

TABLE 2

TRANSMISSION MEDIA

	TWISTED PAIR	BASEBAND COAXIAL	BROADBAND COAXIAL	OPTICAL FIBER
SIGNALS SUPPORTED	Analog/digital; half or full duplex; single channel; one way	Digital; half duplex single channel; two way	Analog/digital; half duplex w/1 channel, full w/2 channels; multi-channel; one way	Digital; half duplex w/1 fiber, full w/2 fibers single channel; one way
MAXIMUM DATA RATE	1 Mbps	10 Mbps	5 Mbps per channel	2 Gbps per fiber
MAXIMUM BANDWIDTH	3 Khz	400 Mhz (1 channel)	400 Mhz (6 Mhz/channel)	565 Mbps
MAXIMUM LENGTH	3 Km	10 Km	50 Km	over 75 Km; exceeds LAN distances
AVERAGE COST	$4.50/m for 200 pair	$3/m	$7/m for 1/2 in; $10/m for 3/4 in	$1/fiber/m for 50/125 micron 1300nm fiber; $20/m for a 30 fiber cable

distance for twisted-pair local area networks is generally three kilometers (3km) and the maximum data rate is one million bits per second (Mbps). A 200-pair cable suitable for outside use will cost about $4.50 a meter.

The finite limits of a transmission path are explained by Shannon's Law, one of the fundamental laws of communications:

$$C = W \log_2(1 + S/N)$$

where C = maximum capacity in bits/second (bps)
W = bandwidth
S/N = ratio of signal power (S) to noise power (N)

This law demonstrates that the limiting factors on transmission capacity are bandwidth, signal power, and noise. As distance increases, signal power decreases, so the transmission capacity will decrease. For a constant bandwidth and constant path length, to increase the data rate, the signal must be compressed. This compression provides less information about the signal and makes signal detection less tolerant of error causing conditions, thus increasing the overall error rate.

The use of coaxial cable allows for greater bandwidth and therefore the capacity for a higher data rate than twisted pair. Because of its shielding, coaxial cable is also more resistant to external noise than twisted pair. There are two main types of coaxial cable: baseband and broadband. Most cable television companies use broadband coaxial cable. Although baseband and broadband are physically similar, they are operationally very different. Baseband systems can only carry one signal at a time and only in a half-duplex mode (one direction at a time). Baseband supports only digital signals and uses repeaters to maintain signal levels. Maximum distances for baseband nets are 10km with a maximum data rate of 10Mbps. A baseband cable plant can only be tapped at certain intervals (based on wavelength). The major advantages are the ease of installation and maintenance. Xerox's Ethernet is a baseband LAN. Ethernet coaxial cable costs about three dollars a meter.

Unlike baseband, broadband cable can support voice and real-time full-motion video, as well as data applications. Use of frequency division multiplexing (FDM) allows broadband to carry more than one signal at a time by splitting the bandwidth into different channels. Transmission is normally half-duplex; full-duplex can be provided by using two channels. As broadband cable transmits only analog signals, radio frequency modems are needed to modulate and demodulate the digital signals. Instead of repeaters, broadband uses amplifiers to maintain signal levels. Use of amplifiers and channelization allows broadband to transmit over greater distances and support more devices than a baseband system. However, broadband cable is more difficult to install and tap than baseband cable. Baseband cable is generally marked where a tap can be made, whereas broadband cable taps depend on the size of the system and the vendor.

Broadband local networks can use either single or dual cable systems. In dual cable systems, signals are transmitted on one cable and received on the other. The cables are joined at a headend to form an open-ended loop. The head-end transfers signals from one cable to the other. In single cable systems, different frequency bands are used for inbound and outbound signals. The headend performs frequency conversion to change inbound signals to outbound signals. If inbound and outbound bandwidths are equal, the system is termed mid-split. A sub-split occurs when the outbound bandwidth is greater than the inbound bandwidth. Cable costs for single cable broadband are half that for dual systems, but the bandwidth, and consequently the potential data handling capacity, is also halved. The installation cost, however, is only slightly higher for dual systems; since cable installation costs are usually eighty percent of the total cost, the cost per channel favors the dual cable system. Broadband systems usually support distances up to 50km at 5Mbps per channel. Broadband coax is about seven dollars a meter for half-inch diameter and ten dollars for three-quarter-inch cable.

Although use of optical fiber for local transmission is new, it has characteristics that may make it the best local transmission medium in the foreseeable future. Fiber is small, lightweight, durable, possesses a greater bandwidth (gigahertz versus megahertz) than other media, and can transmit voice, video, and data. Optical fiber does not require repeaters or amplifiers for local transmission purposes, is not affected by electrical interference, and has emanation characteristics that make it more secure than other media. Transmission rates are limited only by current photonic technology. For a 50/125 (core/cladding) micron cable with twelve fibers the cost is twelve dollars per meter ($1/fiber/meter); a cable with thirty fibers would cost about twenty dollars per meter. Fiber can be used for either baseband or broadband systems. However, the installation and repair of optical fiber requires highly skilled personnel. Fiber is currently the most expensive local transmission media, primarily due to the high cost of electro-optical converters and photonic wave division multiplexers (WDM). The converters transform signals transmitted over copper wire into light pulses that can be transmitted over optical fiber, and vice versa. The multiplexers combine several wavelengths, each capable of carrying a different signal into a single signal carried over the fiber; the process is reversed at the distant end.

2. <u>Network Interface Units (NIUs)</u>

The interface units physically connect local area network user devices to the local area network transmission medium and contain protocols and other software/firmware, not already contained within the user devices, for supporting services on the net (such as file transfer, resource sharing, and protocol conversion). The flow of packets is buffered and managed within the interface units so connected devices can transfer data simultaneously and full duplex at required speeds. NIUs may be self-contained units or may partially reside in the backplane of the supported endpoint object. The self-contained units can have ports to support from one to thirty-two EPOs.

There are three main types of NIUs: terminal, bridge, and gateway. A terminal NIU is used to connect devices like dumb terminals, microcomputers, and peripherals (printers, storage devices) to a local area network. A bridge NIU connects two similar nets. It may connect two baseband networks, two channels on a broadband net, or two broadband local networks. A gateway NIU connects dissimilar networks. Gateways provide connection between a local area network and a long haul network, such as the Defense Data Network (DDN), or between two LANs. A gateway is generally used when transmitting outside a local address group.

3. Network Management System (NMS)

A network management system provides the means to manage the realtime operation, control, and analysis of a local area network. The following functions are supported: initialization and configuration of network resources; controlling access to the network; monitoring performance and operational data; fault detection, isolation, and correction; and managing the security functions of the network.

D. LAN MEDIA ACCESS METHODS

The media access method controls network traffic by determining when and how a user device communicates with other devices. The topology can also affect the choice of media access control method. The primary access methods are token passing and carrier sense multiple access with collision detection (CSMA/CD). In token passing, a control token is passed around among users; the device with the token is the only one that can transmit. Sometimes a slot of time, instead of a token, is passed. Token passing is required for ring topologies and is logical with the star topology.

With CSMA/CD, a device waiting to transmit listens to the channel before transmitting. If another device is transmitting, the one waiting will sense the carrier and wait until the channel is clear. If two transmit at the same time, collision detection stops the transmissions. Each device will wait a random time before attempting to retransmit. CSMA/CD is often used with bus (and related) topologies.

CSMA/CD works best when devices exchange lengthy messages, as this provides the best normalized propagation delay. Normalized propagation delay is the ratio of the time a packet takes to travel through the network to the time necessary to transmit a packet. A ratio of one or less is optimal. As the cable length increases, propagation time and, therefore, normalized propagation delay also increase. The signaling rate is also a factor; as signaling rate increases, the packet transmission time decreases increasing the normalized propagation delay.

E. THE INTERNATIONAL STANDARDS ORGANIZATION OPEN SYSTEM INTERCONNECTION MODEL

The International Standards Organization (ISO) Open System Interconnection (OSI) model is a seven-layer protocol reference model. (See Figure 2.) The levels are physical, link, network, transport, session, presentation, and application, numbered one through seven respectively. It is important to note the components of a local area network only support levels one through four. A brief description of all seven layers follows.

The physical layer defines the physical characteristics required to interface to the transmission medium. It specifies the hardware interface. The Electronics Industries Association (EIA) RS-232C interface is one of the most common physical interfaces today.

Link layer protocols establish a data link across the transmission medium, initialize and control data flow across the link, and terminate the link upon completion of data

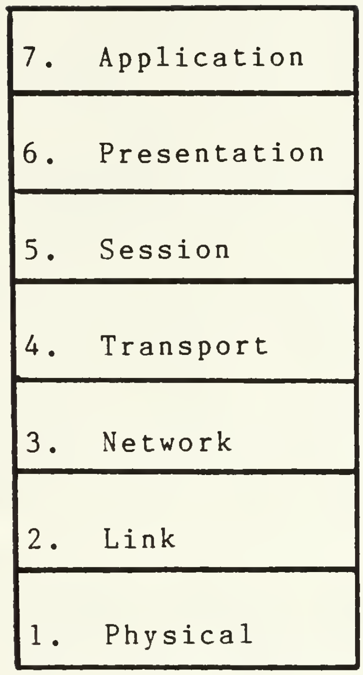

Figure 2 ISO OSI Reference Model

transfer. Error detection and correction are supported in the link layer. High-level data link control (HDLC) is a link layer protocol.

Network connections are established and released in the network layer. Data packet structure, format, sequencing, and routing are also controlled in this level. The DDN X.25 protocol is a common network protocol. The Department of Defense Internet Protocol (IP) is another network protocol.

Layer four ensures data integrity between hosts. It acts as a buffer between levels one through three (communications protocols) and five through seven (data processing protocols). Transport Control Protocol (TCP) is the Department of Defense mandated protocol for the transport level.

The session layer establishes and controls connections between processes on hosts after the transport layer has established the connection between the hosts.

The presentation layer performs code conversions, compresses text, and encrypts data preparatory to data transfer.

User selection of network services is supported at the application level.

Local networks include the physical, link, network, and transport protocols. Each layer is affected by the layers above and below it. The protocols for layers five through seven must support the services the user needs and the LAN protocols must support the upper level protocols. A poorly selected transport layer can cause the most problems for the user.

F. SUMMARY

This section defined a LAN and discussed the capabilities and limitations of its component parts: transmission media, network interface units, and network management system. Local network topologies and media access methods were also addressed. A description of the seven layer International Standards Organization Open System Interconnection model was provided. Local area networks, as defined herein, are composed of the first four layers of the model: physical, link, network, and transport. The top layers--session, presentation, and application--and the endpoint objects are application-dependent and are, therefore, the responsibility of the user.

III. AIR FORCE OPERATIONAL REQUIREMENTS

A. WHAT DOES A LAN REPLACE?

If all users agreed on the definition of a local area network, they might all agree on what a local area network replaces. Some feel the base telecommunications center (TCC) would be replaced by a local network. This is inaccurate; TCC operations would be enhanced by a LAN. For the message handling environment, the local area network replaces the base information transfer service (BITS). BITS is made up of personnel and vehicles, on a base, delivering in hours (or days) paper copies of messages that can be transmitted worldwide in minutes. A properly implemented network would make the printing out and hand-carrying of those messages unnecessary. The messages could be processed and forwarded electronically to the intended recipient.

LANs also speed up some processes. A staff coordination cycle currently consists of an action officer preparing a draft (hopefully on a PC), and hand-carrying it or sending it through distribution for concurrence/approval. If changes are needed, it will be sent back with recommended changes written on the draft. The coordination process can easily be twice as long as the creative process. With the electronic connection provided by a local area network, the draft could be "shotgunned" (sent to many offices at once) for coordination. All the comments could then be incorporated at one time and the draft could be shotgunned again. Besides saving time for everyone involved in the process, electronic coordination would save resources (paper and ink).

A local area network cannot replace anything, however, if potential users have social and psychological barriers to computers and electronic transmission of information. Some people feel better with a notebook, filing cabinets, and libraries than with a keyboard, a box of computer disks, and a modem. Fortunately, education can remove the barriers and retirement will remove those who cannot overcome them.

B. WHAT ADDITIONAL SERVICES WILL A LAN SUPPORT?

A broadband system can do more than provide data connectivity between computers. Video capabilities of broadband cable, as demonstrated by the cable television industry, are well known. Both analog and digital voice transmission can be supported on a broadband system. The same cable that supports data, voice, and video can provide channels for alarms and sensors. Significant cost savings can be achieved using the same physical cable plant for many uses instead of installing separate cable plants for each use; this can be a significant selling point to a potential user.

For users who want only to speed up current office tasks, the general availability and supportability of a baseband system has many advantages, discussed elsewhere in this paper.

C. WHAT A LAN ISN'T

By now, the reader has probably noticed the phrase "the LAN will support" instead of "the LAN will provide." As explained earlier, a local area network only addresses layers one through four of the ISO OSI model. The higher levels, notably the application level, are not considered part of the network. The local area network is like an engine. The higher levels are equivalent to wheels. Neither alone is able to do anything. The short definition of a LAN, a smart transmission path, says it all. No one expects a piece of wire to provide electronic mail or file transfer. A network by itself, is not capable of electronic mail or maintaining a calendar.

A local area network is not the user devices attached to it, nor does it include the applications software used with it. Explanations of the services supported by a LAN invariably describe services that require workstations and special software. The devices and software, along with the network, are part of an information system. Office information systems (OISs) do include the devices, software, and connectivity (the local network). A given OIS may use only one channel of a broadband network. A single physical broadband cable plant can support many logical networks. Therefore, many OISs can exist on a single LAN.

D. REQUIREMENTS

User requirements are varied. A primary requirement is to have a single workstation or microcomputer which can provide the user with access to the other users and processes supported by the local area network--replace the "air gap." A wing commander may require access to every database on the installation. A command post would require such access to support contingency operations. Command and control is not supported by having many terminals hardwired to as many mainframes; it is best supported by having a robust network that allows a single terminal access to many mainframes and databases.

Flexibility is another requirement. The network management system should be able to reconfigure the system to support physical relocation of any user community. A tornado destroyed both the air traffic control tower and the command post at Altus AFB, OK, in May 1982. The alternate operating location for both functions was the alternate command post. Because the alternate command post could not physically support both functions, air traffic had to be controlled from the cockpit of a C-141 until a temporary tower was ready. If the command post functions could have been relocated to some other office, air traffic control operations could have taken place in the alternate facility. Relocation and reconfiguration flexibility is a major advantage of a LAN.

The AFLANSPO conducted a survey in 1983 of potential local area network users. (See Appendix C.) The survey dealt with the following areas: applications which need data communications; numbers of devices to be networked, current and future projections; mobility requirements; connectivity among different types of devices; requirements for access to long haul networks; security requirements; and survivability requirements.

The survey results showed a wide variety of applications that would require data communications. These applications included word processing, electronic mail, document distribution, and video conferencing.

The survey also showed that the number of devices requiring network connectivity was expected to increase every year. The networking scheme would have to support the periodic relocation of devices, as well as the growth in the number of devices on the network.

User responses showed a need for connectivity between a variety of devices (terminal to host, host to host, workstation to workstation) as well as connectivity between devices from different vendors. Connectivity through the local net to devices that could only be reached over a long haul network was also required.

Security was a major concern of potential Air Force local network users; eighty-six percent indicated a requirement for handling classified data. Survivability was also important to those surveyed, as many of the nets would support command and control, and combat operations.

E. SUMMARY

The current state of local area network technology can accommodate a wide variety of user requirements, but it cannot support existing requirements for security and network management. A well-designed local area network must provide access to all the data required for job performance from a single terminal. It must have the flexibility to support future growth and reconfiguration while maintaining a high degree of reliability. Continued education is needed to ensure maximum functionality of the users' networks.

IV. PROBLEMS IN IMPLEMENTING A STANDARD AIR FORCE LAN

A. CONCEPT

The original ULANA concept was to meet every requirement at every Air Force installation with the same network. Every base would have a large broadband local network capable of supporting 10,000 users. The family of network interface units would be able to support every Air Force owned or leased endpoint object (EPO). The primary advantage of this approach was it would have provided a single system for users to learn. Once a user had been connected to any Air Force LAN, he would be able to operate at any Air Force location with no retraining. Although this approach would probably satisfy most Air Force requirements, there were major disadvantages.

B. COST OF CONNECTION

Interpretation of Air Staff guidance on use of protocols led to a design that included Transmission Control Protocol/Internet Protocol at the network interface unit; this would place a substantial economic penalty on users with dumb terminals to be connected to a mainframe, for users whose PCs are treated like dumb terminals by their network, and for users whose PCs could incorporate the protocols internally. These three categories of users form a very large segment of the potential Air Force local area network community.

Inclusion of TCP/IP at the NIU could double or triple the cost of the terminal and bridge NIUs. Instead, I think these protocols should be implemented at gateway NIUs and at host computers serving as gateways to other networks. Terminal NIUs can be cards that are inserted into slots on some PCs; these cost about $500 each. TCP/IP, when available in this format would add about $1000 to the price. Other types of terminal NIUs are boxes that have two to thirty-two ports. Bridge NIUs can also be boxes; they usually link two to four channels (on a broadband net) or similar networks (for baseband). Implementing TCP/IP in a "box" NIU costs from $1000 to $2500 per box. Although implementing TCP/IP at a gateway is more expensive (about $5000), the cost per device served is less.

C. FUNDING

It is nearly impossible to implement a base wide local area network on an Air Force base because of arbitrary funding rules. A major command (MAJCOM) will "own" the base and be the host. However, every base has tenants from other MAJCOMs. These commands control their own funds for base level communications and ADP. A host will not normally want to pay for, nor be funded to provide connectivity for a tenant. A potential solution to this problem would be to have Air Force Communications Command (AFCC) centrally manage all funds earmarked for local area networks since AFCC is tasked with implementing local area networks for the Air Force. Despite the apparent efficiency of this solution, it was not approved by Air Staff; consolidation of LAN funds would have created a large target during the budget process and AFCC, as a support (vice operational) command, has a poor track record of defending budget cuts.

As an alternative a requirements contract is being pursued. A requirements contract is a contract set up for use by many organizations buying the same thing at different times. The major advantages of this type of contract are the lower cost per unit because of the larger purchase quantity, the speed of acquisition since implementers can order from the existing contract and do not have to recompete every implementation, and the standardization allowed when items are purchased from the same vendor. Also, if a requirements contract exists, its use is mandated for all applicable acquisitions.

AFCC has to implement local networks with money provided by MAJCOMs and only for particular portions of a base. Because of the time it has taken the AFLANSPO to develop standards, no requirements contract for LANs exists; therefore, the implementations are done on a case-by-case basis. If AFCC cannot meet a command's required operational date, that command may bypass AFCC and contract out the effort itself. While this approach may satisfy immediate requirements, it has led to a proliferation of many small networks and diverse equipments outside AFCC's control, but which AFCC may eventually have to operate and maintain (O&M) with in-house or contracted personnel. Work is progressing within the Air Force to get LAN requirements and O&M contracts which will provide timely implementations and standardized, supportable local area networks.

D. ADP VERSUS COMMUNICATIONS

Within AFCC, ADP and communications are treated the same. However, the General Services Administration (GSA) keeps the two categories strictly, if arbitrarily, separate. ADPE purchases require submission of a request to GSA for a delegation of procurement authority (DPA). The DPA process can add a month or more to the acquisition cycle. GSA has stated that LANs and LAN components are ADPE. In the case of a requirements contract, once the DPA has been obtained, the problem is solved. An additional month for the case-by-case acquisitions is more serious. A single month's delay can result in the loss of funds by moving an acquisition into the next fiscal year.

E. AVAILABILITY

A further disadvantage of the original ULANA approach was that it did not use commercially available products. The single-style Air Force local area network required significant research and development expenditures--and time. Many users did not wait for ULANA to develop Air Force standards, but bought their own local networks. As a result, AFCC set up an Implementation of Local Area Networks (ILAN) office in an effort to direct LAN acquisitions towards the evolving ULANA standards. Since there was no requirements contract, procuring a local area network was done on a case-by-case basis and could take up to eighteen months. The advantage to the user was the guarantee of maintenance for the network.

F. TYPICAL INTERCONNECTION SCENARIOS

How does one apply the above knowledge of topologies, access methods, and operational requirements to provide a design satisfactory to the user? Is a unique military solution necessary or superior to designs available commercially? Three typical connectivity situations and potential solutions will be outlined below to demonstrate a design process. (See Appendix D.) The first example will be a small office environment. The other two will be large organizations, one with all (or most) members in a central location, the other with its members dispersed over a fairly large geographic area. The size of the organization should be the first consideration, then other requirements can be taken into account.

1. Small organization

A small organization could be the base legal office or a semi-autonomous section of a larger organization. This simplified example will use three adjacent rooms on one floor of a building. One room will house the division chief and division secretary and there will be a four person branch in each of the other two rooms.

Each person has an IBM PC compatible microcomputer; the division secretary has an IBM PC/AT compatible computer (multitask personal computer). Each branch and the division chief have a draft quality printer. The secretary has a letter quality printer and produces the final copies of all documents.

The multitask workstation has a large (50Mbytes or more) magnetic storage unit (hard disk drives or Bernoulli box). All division work is stored here when completed or ready to be sent out; data on the storage unit is backed up weekly.

It is possible to rely on air-gap connectivity for such a small organization. However, with individual storage plus storage at the multitask workstation, it will be possible to move to an electronic filing environment and an electronic mail environment. The e-mail environment will also allow information exchange outside the division.

There are two problems to be solved: how to hook up the ten PCs and four printers to each other and how to provide this OIS access to other networks.

A star topology, using the multitask workstation as the central point, could be used. A polling system would allow the other PCs to request services, primarily to use the printers, pass files to the secretary, and for access to e-mail. Some disadvantages to this would be the multitask workstation as a single point of failure, having to run wiring from each PC and printer to the multitask workstation, and having to send a request for access to a printer in the same room.

A token passing ring would be a better solution, especially in such a small organization. It would not require as much wire and requests for printing could be sent directly to the desired printer. This has the added advantage of allowing a PC other than the secretary's to directly use the letter quality printer.

The multi-task workstation should be used as the connection point to outside networks for both solutions described above. Although a malfunction with this workstation would prevent connection to another network, it is the most flexible solution when the type and location of gateways to other networks is unknown. This is also the most cost effective as the organization will only have to

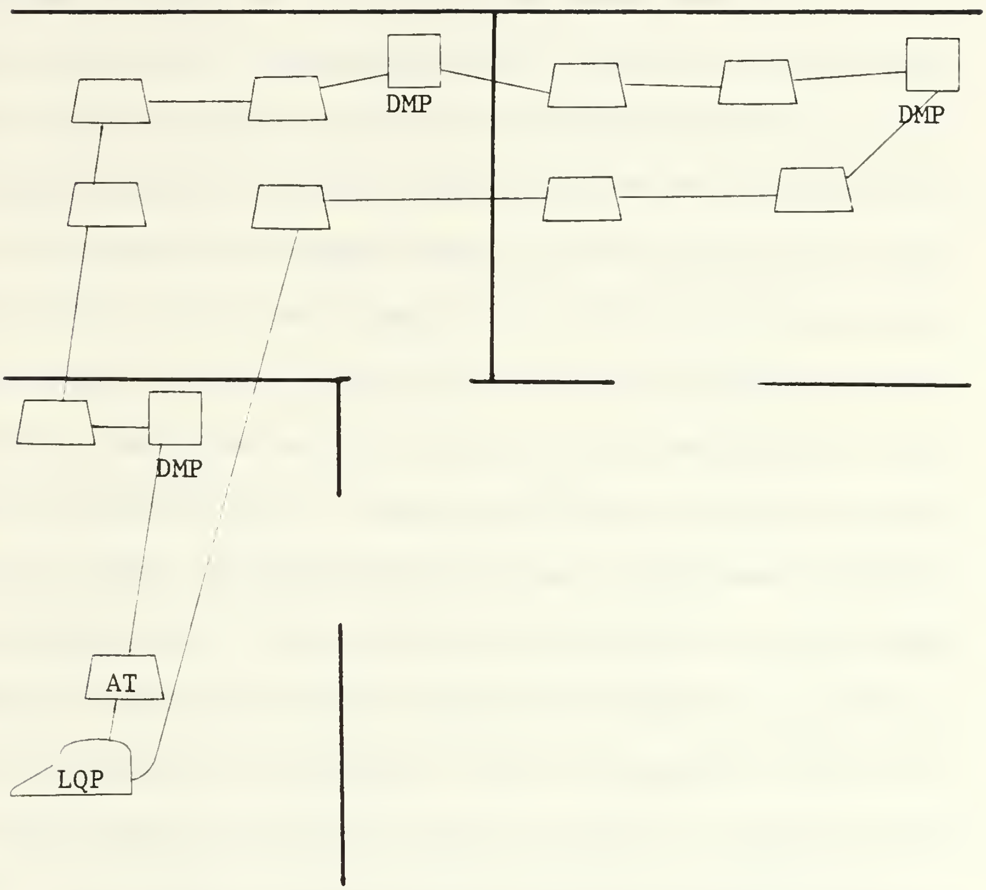

Figure 3 Token Passing Ring for a Small Office

implement the Air Force protocol standards for a single workstation, not all ten of them. (See Figure 3.)

2. Large, geographically concentrated organization

For purposes of this paper a large organization is one with more than a hundred people. For this example, the large, geographically concentrated organization will have 500 members and be housed in a single three story building. There are 100 people on the first floor and 200 on each of the other two floors. The goal is to have a PC for every member of the organization, but right now there are seventy-five PCs on the first floor, 100 on the second floor and seventy-five on the third floor. Some of the PCs do not use an IBM-compatible disk operating system (DOS) and will be replaced as funds permit; therefore, the documents on them must be converted for use on a DOS-based PC. There are two mainframe computers in the building and both can be hooked into a nearby terminal access controller (TAC) for DDN access. The mainframes host several application programs and can act as servers for the PCs.

To solve this problem it, too, must be broken down into its component parts. A continuing problem, until all the microcomputers use the same operating system, is sharing documents between computers with incompatible operating systems. Translation at a host computer would be the optimal solution. If this is not possible, an interim solution would be to use a communications application program to move documents between operating systems. This would require "manual" translation of some control characters in the documents, but is generally preferable to retyping the documents. In both cases, the connections that support the net will also support the document translation.

The other components of the problem are connecting all the endpoint objects and supporting the desired increase in EPOs. These must be broken down into the same level of detail provided in the analysis of the small organization. Location of EPOs and direction of information transfer are the important considerations in providing an adequate solution for this building. If each floor is fairly autonomous and the information transfer is primarily within each floor, then each level of the building could be treated separately with information transfer between floors going through the mainframe computers. However, for this analysis, the organization in the building is a hierarchical one and the upper levels of the organization are housed on the first floor. Subordinate levels (divisions and branches) are on the second and third floors. Therefore the information transfer within each deputate of the organization must travel between floors. There is also a significant amount of communication between counterparts in different deputates.

If there were four or fewer deputates within the building and no significant growth planned, it might be feasible to use a star configuration for each deputate, tie each one to a mainframe, and allow the mainframes to provide connection between the deputates of the main organization. In our example, however, the organization has eight deputates and a goal to double the number of devices, so the star configuration is not feasible.

If each deputate was located in the same section of the building (even though on different floors) and there was a limited growth requirement, each one could be connected by a token passing ring. This could be an inexpensive solution if the building was prewired with datagrade twisted-pair wire and there was spare capacity. Each ring would be connected to a mainframe which would provide internetwork communications: to the other deputates, to local area networks on the installation, and to long-haul networks. The rings should be dual rings so that a single break in the ring will not bring the network down; this will allow breaking the ring to add EPOs without bringing the network down. A major advantage of this solution is that it is commercially available (IBM Token Ring, Z-LAN) with network management. However, this solution does not support the peer traffic between deputates as the host computers will become a chokepoint for all internetwork information transfer.

A tree topology using carrier-sense multiple access with collision detection (CSMA/CD) over broadband cable is a

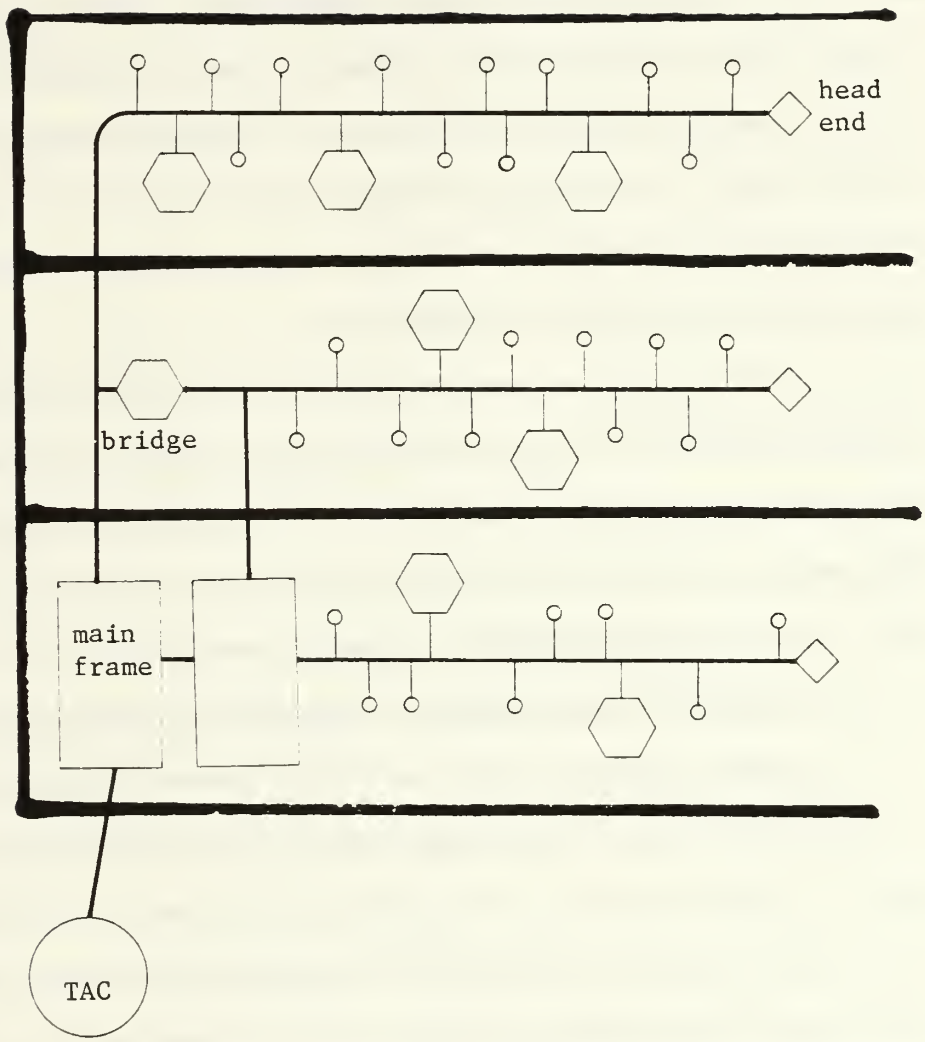

Figure 4
Intrabuilding Broadband Tree for a Large Organization

better solution for this organization. This type of network will provide each deputate with its own virtual OIS by giving each their own channels. Intradeputate traffic would stay on the same channel while interdeputate information would switch channels at a bridge NIU. Extra head-ends and a dual cable system would ensure enough bandwidth for the anticipated increase in devices. Use of gateway NIUs would allow direct connection to the DDN TAC, if required. The disadvantage of this solution is the limited network management currently available.

In the above solutions, a case can be made for implementation of TCP/IP only at the host computers because they provide the organization's interface to other networks. The gateway NIUs in the tree local area network would also have to implement TCP/IP. (See Figure 4.)

3. <u>Large, geographically dispersed organization</u>

This example will be a 400 person organization spread in several buildings over an Air Force base. The base is about three miles square (1.75 by 1.75 miles). The organization is an engineering group formed from the consolidation of six smaller units. Each unit had its own buildings and no relocation took place after the larger organization was formed. There are three fifty person sections, two twenty-five person sections, and one 200 person section. The largest section takes up four buildings of a six building complex. One of the smallest sections is in another building of the complex, and the other one is in a solitary building half a mile away. The remaining three sections each have their own building and are located within 500 yards of each other in a fairly populated area on the base. These three sections are about half a mile from both the largest and the most isolated sections.

The largest section writes technical manuals, test procedures, and reviews statements of work for technical accuracy. Members of this section also participate in test and evaluation teams for communications systems. The small isolated section has a classified mission and also requires access to most of the documentation produced by the other sections. The mission of the section collocated with the largest one is computer chip and integrated circuit design. The other three sections perform the same mission for different types of equipment: install, train, and provide contingency engineering support. Part of this mission is classified, but the travelling associated with the job requires much administrative support.

All the administrative functions of this organization are supported by IBM PC compatible microcomputers in each section. For some sections, the computers are TEMPEST certified to prevent unwanted emanations. The integrated circuit section has a computer assisted design (CAD) system in a vault; this system is not compatible with the IBM PC, but can be linked over an

Ethernet to IBM and compatible PCs. The organization does not expect to add many endpoint objects but ultimately requires a multilevel secure network to support both the classified and unclassified portions of its mission.

The organization's goal is to electronically link its dispersed units in such a way that the network will support multilevel security when it becomes available. Dealing with future capabilities is much more difficult than dealing with future growth and requires a careful analysis of the current and projected information paths. The isolated section only requires connectivity to the largest section for documents and to a multilevel secure gateway (when available) for access to Department of Defense secure networks. The other sections require access to each other and to a multilevel secure gateway when one becomes available. Reliability of the network and the gateways is critical to the mission.

A mesh topology will be used by this organization to support its reliability requirement--there will be at least two paths between any two sections and at least two gateways any section can access. Optical fiber will be used for all interbuilding connections. This will prevent electrical emanations when the network is able to send classified traffic. The disadvantage of this network will be the price. Because of the cost, the group's local network will have to evolve. The topology will evolve from a tree to mesh in order to support multiple paths between sections and gateways. The network will evolve from connected baseband nets into a broadband network to take advantage of both existing network management capabilities and current local transmission capabilities over optical fiber.

Each section will start with a baseband net most appropriate for its size and pattern of information transfer. No EPOs meeting TEMPEST criteria or in a vault can be connected to any network until the required security is available. Therefore, the largest section will get the first local area network, followed by the three installation sections. The administrative area of the microchip section can probably be served by the large section's network. The isolated section can hand carry disks over a long air-gap until it gets a network.

The interbuilding links should be multiple-fiber cables. Then, each baseband network can operate on its own fiber which will reduce costs of electro-optical components; only one section will be sending traffic over a given fiber, so only one light source will have to be modulated and demodulated on each fiber.

The first link installed should go from the multi-building complex to one of the three installation sections. The next links should connect the the buildings within the multibuilding complex and then the three close buildings. The second long link should be between the

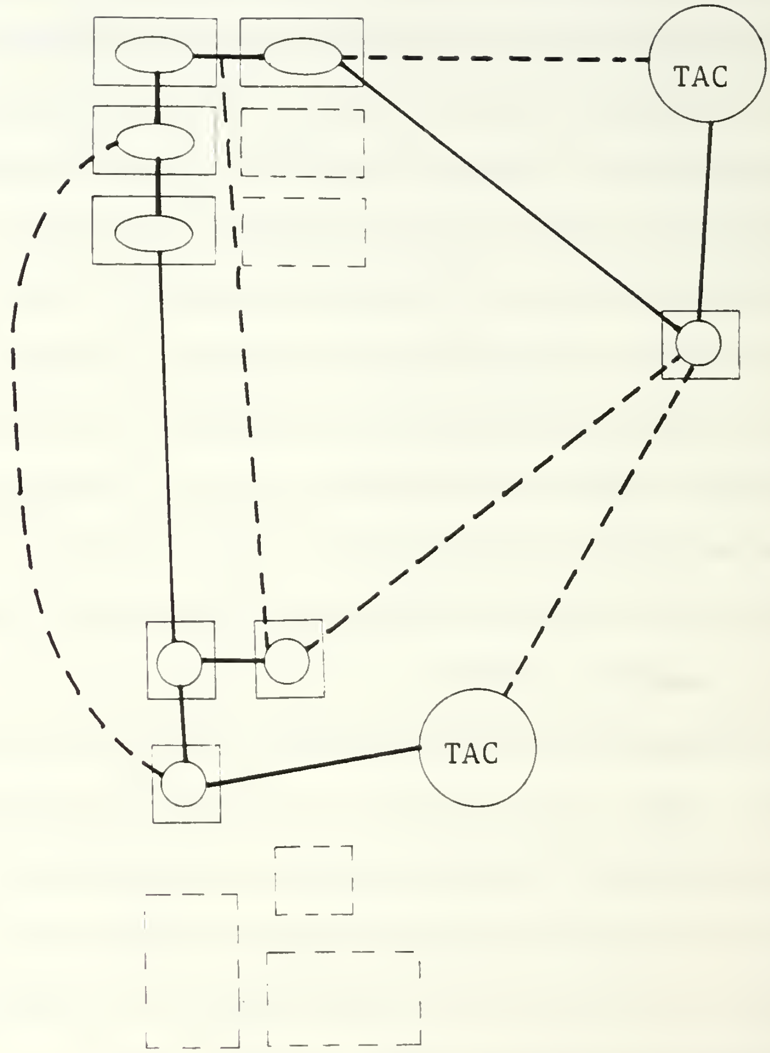

Figure 5
Interbuilding Mesh for a Large, Dispersed Organization

complex and the solitary building. As funds permit, additional long links should be installed until each of the three close buildings is separately connected to the complex and the solitary building is connected to one of the three close buildings. As the network evolves, it may be possible to sell any extra capacity to other users on base.

It may be necessary to purchase a mainframe computer to host application programs and to act as a gateway between the initial networks. Careful planning will allow this host to continue as an applications server and to provide network management for the goal network. (See Figure 5.)

G. SUMMARY

Most problems plaguing local network implementation can be traced to funding, lack of central control, and absence of a standard method for procuring local area networks. Support commands' (AFSC and AFCC) efforts in establishing standards have not been fast enough to support the operational commands, leading to a proliferation of potentially unfunctional and hard-to-maintain local area networks.

Three representative connectivity problems that can be solved by a local area network were described. Solutions using available technology were then proposed.

V. RECOMMENDATIONS

A. INTRODUCTION

A brief overview of local area networks has been presented. The discussion covered basics of local area networks, Air Force requirements, and problem areas. A pragmatic, commercially available solution will be proposed. The Air Force is currently developing a requirements contract for LANs and LAN components. Once the contract is in place, all commands will have to use it. They'll be willing to do so because it will be the quickest way to get a local area network. As previously stated, a requirements contract minimizes both the funding problem and the DPA issue.

The recommended solution is an alternative to the original ULANA concept of a single AF LAN. My solution sacrifices total standardization for commercially available products that will support users now. Instead of a single type of LAN, the tailored LANs will allow a choice from a set of standards.

My solution supports implementing TCP/IP as close to the endpoint objects as feasible economically. Gateways must implement TCP/IP and some bridges should implement these protocols. As TCP/IP board and chip costs decrease, implementation at every endpoint object may become cost effective.

B. DESIGN

As shown above, no single design is suitable for all users, so a single design should not be mandated or used. A careful analysis of local user requirements should be made before a network design is selected. The network selected must support the current and future needs of its users. The analysis should identify the following: mission and organizational structure to be supported; physical locations to be connected; types of computers and peripherals to be connected; existing host processor and terminal locations; equipment and organization relocation; security, survivability, and reliability requirements; types of communications (internal, lateral, or hierarchical); number of users within a particular user group; and required data transmission rates.

To meet all requirements, a base should have a broadband backbone which connects networks. Each user group will have the type of LAN that best supports it. A base would then have a fiber backbone with branches of broadband coaxial cable, baseband coaxial cable, twisted pair, and optical fiber. The backbone could also be broadband coaxial cable. A user group would then be able to use the topology and

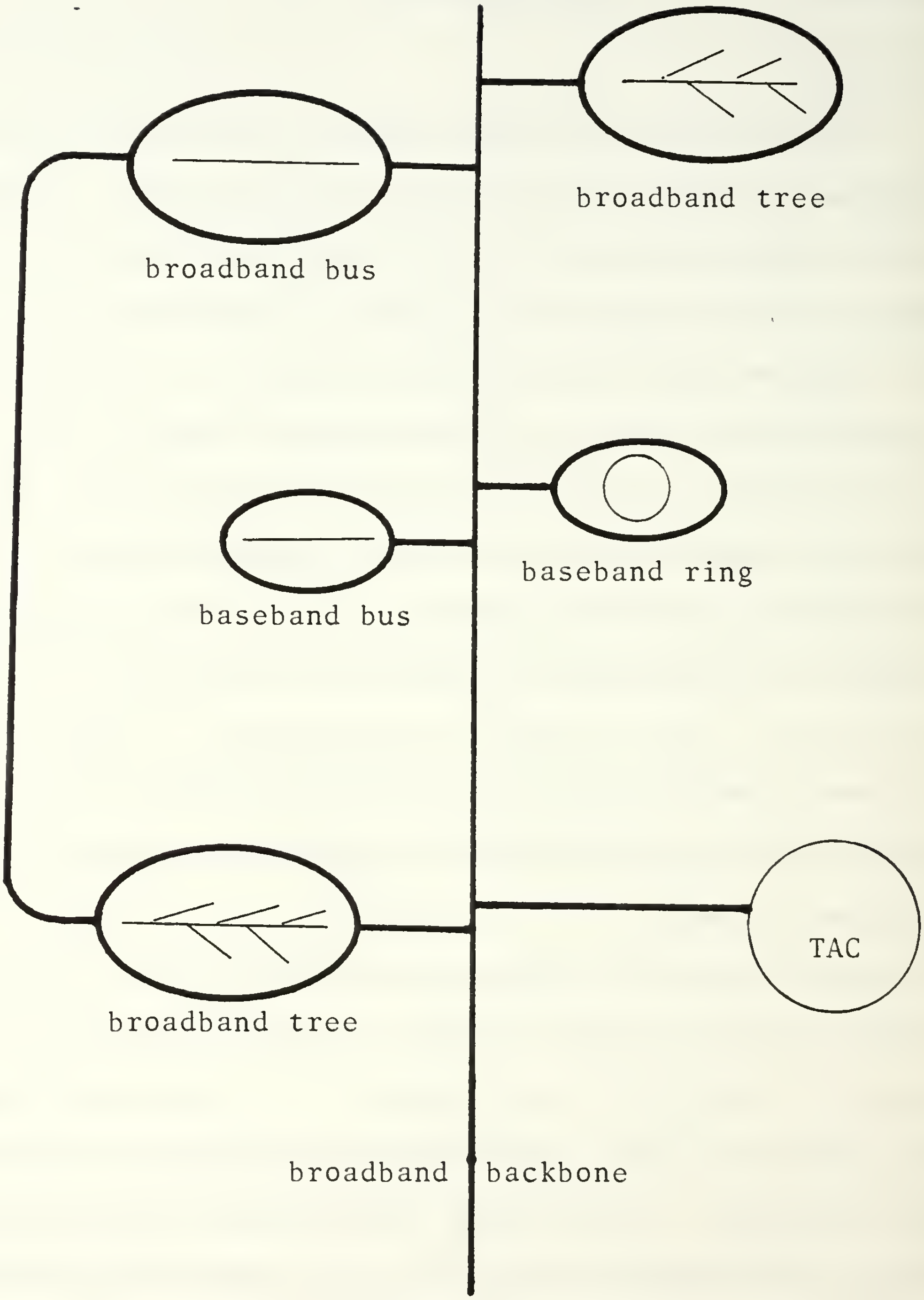

Figure 6
Potential LAN Solution for an Air Force Installation

access method that best meet its requirements and budget. (See Figure 6.)

C. IMPLEMENTATION

Successful implementation depends on availability of requirements contracts. To maintain fair and open competition, each type of local area network should be awarded a separate requirements contract. An alternative would be teams of contractors bidding on an all-inclusive local area network requirements contract. With such contracts in place, a requirements analysis would be accomplished by the ILAN office and the appropriate components for the design would be ordered and installed. A broadband backbone will have to be provided as part of the base cable plant; the host command and AFCC should fund the backbone, since it will provide service for every element on the base.

A research and development contract must be let to develop a network management system that works with products from multiple vendors and can manage many subnets (including those that have proliferated while standards were being developed). Then, O&M of the base level network can be conducted from a single location by AFCC personnel. For reliability and survivability, network management subsystems can be used, providing graceful degradation of the system.

Each subsystem would provide data to the NMS automatically, but could be manned if the NMS failed.

D. SUMMARY

A strategy for local area network design and implementation for the Air Force has been proposed: use of commercially available local network technology implemented through requirements contracts. The strategy supports Air Force requirements for connectivity and flexibility and can be procured under current funding policies.

This thesis was motivated by the AFLANSPO. ULANA is a research and development program attempting to design a single standard local area network to satisfy all Air Force requirements. Although the goals are admirable, the time taken to develop the standards has permitted the proliferation of nonstandard local area networks. Selection of a subset of commercially available products will satisfy the majority of users while reducing the O&M problems.

APPENDIX A

DEFINITIONS AND ABBREVIATIONS

ADPE - Automated data processing equipment

AFCC - Air Force Communications Command

AFSC - Air Force Systems Command

AFSC - Air Force Specialty Code; designator of skill an Air Force member possesses

AFLANSPO - Air Force Local Area Network Systems Program Office; part of Air Force Systems Command's Electronic Systems Division at Hanscom AFB, MA

Architecture - Design principles, physical structure, functional organization, data format, operational procedure, and other features used as the basis for the design, development, and operation of a user application network

BITS - Base information transfer service; intrabase courier service

CSMA/CD - Carrier Sense Multiple Access with Collision Detection; a LAN access method

DPA - Delegation of Procurement Authority; from GSA granting authority for a particular acquisition to another agency/organization

EPO - Endpoint object; device connected to a LAN such as a computer, printer, or storage device

FDM - Frequency division multiplexing; the available transmission frequency range is divided into narrower bands each used as a separate channel

Full-duplex - Capability to transmit and receive data at the same time; able to transmit across a line in both directions at the same time

GSA - General Services Agency

Half-duplex - Able to transmit only or receive only at a given time; capable of transmitting across a line in only one direction at a time

IP - Internet Protocol (MIL-STD-1777)

ISO - International Standards Organization; established in 1947 to promote development of standards in computer technology, US representative is ANSI

LAN - Local area network; a smart transmission path used to support applications such as file transfer and electronic mail

Layer - A group of related functions that comprises one level of a hierarchy of functions

MAJCOM - Major command (i.e. AFCC, Strategic Air Command, Military Airlift Command, AFSC)

MIL-STD - Military standard

NIU - Network interface device; provides connection to a LAN

NMS - Network management system; provides realtime configuration and control of network

OIS - Office information system; a system that includes hardware and software to automate office functions

OSI - Open Systems Interconnection; seven layer protocol model developed by ISO to support LAN standards

PABX - Private automatic branch exchange; computerized switching equipment capable of switching analog and digital signals

PC - Personal computer

Photon - A quantum of electromagnetic energy

Photonics - Use of photons instead of electrons for signal transmission; optical fiber has a greater bandwidth than any electronic transmission medium

Protocol - Rules for communications system operation that must be followed if communication is to be effected; designed to control the layers of a communications network or to control the exchange of data among computers in a network

TCC - Telecommunications center

TCP - Transmission Control Protocol (MIL-STD-1778)

TEMPEST - An unclassified short name for investigations and studies of compromising emanations

ULANA - Unified Local Area Network Architecture; being developed by the AFLANSPO to provide LAN standards for the Air Force

WDM - Wavelength division multiplexing (photonics); the multiplexing of lightwaves in a single transmission medium such that each of the waves are of a different wavelength and are modulated separately before insertion into the medium; WDM is the same as FDM applied to visible light frequencies of the electromagnetic spectrum

APPENDIX B

TEXT OF HQ USAF/SIT 012200Z SEP 84 MESSAGE

SUBJECT: Policy for Implementation of Data Communications Protocols

REFERENCES:

A. USDRE Memo, Host-to-Host Protocols for Data Communications Networks, 23 Dec 78.

B. ASD(C3I) Memo, Host-to-Host Data Communications Protocols, 3 Apr 80.

C. USDRE Memo, DoD Policy on Standardization of Host-to-Host Protocols for Data Communications Networks, 23 Mar 82.

D. USDRE Memo, Defense Data Network (DDN) Implementation, 10 Mar 83.

E. USDRE Memo, DoD Policy on DDN Protocols, 14 May 84.

F. HQ USAF/XOK/ACD Message, 191245Z Apr 83, Policy on Protocols for Packet-Oriented Local Area Networks.

G. DCA/DCEC (R130) Memo, Data Communications Protocol Standards Area Program Plan, 16 Jul 84.

H. Draft DoD Protocol Reference Model, 2 Dec 83.

I. Draft Security Annex to the DoD Protocol Reference Model (U), (SECRET), 21 Nov 83.

J. DoD Standard Internet Protocol, Jan 80.

K. DoD Standard Transmission Control Protocol, Jan 80.

L. MIL-STD-1777, Internet Protocol, 12 Aug 83.

M. MIL-STD-1778, Transmission Control Protocol, 12 Aug 83.

N. MIL-STD-1780, File Transfer Protocol, 10 May 84.

O. MIL-STD-1781, Simple Mail Transfer Protocol, 10 May 84.

P. MIL-STD-1782, TELNET Protocol, 10 May 84.

Q. BBN Report 1822, Specifications for the Interconnection of a Host and an IMP, Dec 81 Revision.

R. DDN X:25 Host Interface Specification, Dec 83.

S. FIPS Publication 100/FED-STD-1041, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Operation with Packet-Switched Data Communications Networks, 6 Jul 83.

T. DDN Subscriber Interface Guide, Jul 83.

U. WWMCCS Host to Front End Protocols: Specifications Version 1.0, 5 Nov 79.

V. AF/SIT Letter, USAF Use of the DDN, 22 Jun 83.

1. SUMMARY. This message provides an overview of data communications protocols, the evolving DoD protocol reference model, DoD standard protocols, and reiterates and affirms Air Force policy on the mandatory use of DoD standard data communications protocols. It is intended to provide a common basis of understanding of the role of data communications protocols in information systems architectures and the importance of standardized protocols in achieving flexible and adaptive systems capable of sustaining mission essential services under stress. This information should be given wide dissemination to include acquainting functional users of information systems with the concepts and policies.

2. DATA COMMUNICATIONS PROTOCOLS.

A. Improvements in electronic technologies, exemplified by the advent of inexpensive and powerful microprocessors, are restructuring the application of information systems across the Air Force. These improvements are promoting the evolutionary growth of distributed (decentralized) and specialized information systems capabilities. This evolution offers significant potential to achieve information systems which are more responsive to mission and command requirements. For example:

(1) Robust systems capable of sustaining essential functional capabilities while subjected to significant levels of stress.

(2) Specialized of functionally-dedicated subsystems optimized to extend the abilities to meet demanding user applications.

(3) Controlled resource sharing which extends the scope of functionality available to a wider group of users while maintaining privacy/security controls.

(4) Graceful incremental evolution and capabilities to rapidly accommodate additional users, system upgrades, and new services.

(5) Adaptation to the leadership style and support requirements of commanders.

(6) Enhanced timeliness, accuracy, efficiency and cost-effectiveness of information systems.

B. To achieve the full potential of these evolving information systems--particularly the level of flexibility required to provide survivable and enduring information systems support--a corresponding growth in the level of controlled interconnection and interoperability of information systems and subsystems is essential. Consequently, there is an accelerating demand for high-speed telecommunications and interoperable information system architectures. Improvements in relatively inexpensive high bandwidth local telecommunications (e.g., coaxial and fiber optic cable transmission systems) and the proven efficiency of packet switching technologies have supported these demands.

C. Exchange of information among information systems is a complicated process. The required cooperation must be formalized in rules which define the methods, procedures, and conventions (to include syntax and semantics) for carrying out the exchange. These rules are called protocols and are embedded in particular implementations within the information systems elements. Protocols are required not only to effect the movement of information but also to insure mutual understanding.

D. Protocols are explicitly or implicitly contained within the information systems architectures. Vendors have tended to deal with protocol issues independently. This has given rise to differing approaches which are often proprietary and generally incompatible. However, growth in the use of, and dependence on, automated information processing; requirements for interoperation of distributed elements; and costs/inefficiencies associated with dealing with numerous incompatible protocol architectures have highlighted the need for standardization.

E. Due to the complexity of data communications, the problem must be approached in a structured fashion which subdivides the issues into manageable portions. This resulted in a concept of a layered hierarchy of protocols. Each protocol layer interacts with its corresponding (peer) layer located in the other information system elements. However, this interaction generally requires support services from a lower layer. Further, each protocol layer's implementation of its services is intended to be independent of the other layers' implementations except for the input/output exchanges (interfaces) which occur between layers to either request a service or respond to such a request. In this manner, protocol development and implementation can be done relatively independently and a modification in the implementation of one layer (that is, of one or more of its protocols) provided that the services offered remain the same and the input/output characteristics (interfaces) are not altered. Peer-level protocol implementations in the different information systems elements need not be identical, as long as the implementations conform to the protocol conventions to achieve interoperability.

F. However, in order to implement this concept there must be a determination made as to the functions to be provided by the protocol hierarchy, and an allocation of subfunctions to a defined set of layers and protocols within the layers. This is the principal purpose of a protocol reference model.

G. There are two efforts to develop protocol reference models. The DoD is formalizing a reference model which evolved from protocol development associated with the ARPANET. In addition, subsequent to much of DoD's development, the International Standards Organization (ISO) began development of a reference model for Open System Interconnection (OSI). (NOTE: An "open system" is one which complies with the OSI model and OSI standards to facilitate interprocess communications.) Both the DoD and ISO reference models are structured to provide services through a layered hierarchy. It is DoD and Air Force policy to make maximum use of international and commercial standards consistent with mission requirements. The DoD is working with the National Bureau of Standards (NBS) and standards bodies to influence standards developments to address military requirements (e.g., survivability and security). To the extent that these efforts are successful, the DoD reference model and protocols will converge with the international and commercial standards.

3. DOD PROTOCOL REFERENCE MODEL.

A. To achieve required flexibility, security, survivability and endurance to satisfy military requirements, the DoD reference model is governed by a set of fundamental principles which include:

(1) That a common internet protocol be used in all networks which intercommunicate. (NOTE: Since the dynamics of warfare, crisis requirements, short-notice mission changes, and flexibility required to support restoral, recovery, and reconstitution will alter the functional requirements for intercommunication, it is a fundamental Air Force goal to provide the capability for intercommunication between all networks--and between elements within networks. Security and privacy requirements will dictate use of procedural restraints, to include technical safeguards, to functionally limit the exercise of this intercommunication; however, the technical means for intercommunication must be in place to sustain essential mission support and adapt to changing mission requirements.

(2) That higher-level protocol groups should have minimum dependence upon properties of subnet services. (NOTE: The peacetime or normal day-to-day characteristics or services of networks may change dramatically under stress (e.g., damage, degradation resulting from inability to adequately maintain the network due to stress-related logistic or personnel restraints, increased congestion due to crisis loading or loss of network elements, longer traffic routes to bypass network damage or compensate for congestion).)

B. The DoD reference model employs a hierarchical layering. The layers (levels) are aggregated into groups to provide a means of describing similar features.

(1) Application Protocol Group: Provides functionality specific to a particular application.

(A) Application level, containing protocols that directly provide the distributed information services appropriate to an application and to its management.

(B) Presentation level, containing protocols that perform virtualization of data representations and shared resources.

(2) Process-to-Process Protocol Group: Provides ability to transfer data between processes running on hosts connected by an internet (to include hosts on same network).

(A) Session level, containing protocols that help to coordinate use of multiple transport services, as well as provide name servers and access controllers.

(B) Transport level, containing protocols that provide for process-to-process communication across one or more networks.

(3) Internet Protocol Group: Provides the ability to transfer data between hosts connected by an internet (to include hosts on the same network).

(A) Internet control level, containing protocols that perform management functions for the internet.

(B) Internet level, containing protocols that perform routing between networks, supplying host-to-host data communications service.

(4) Network Protocol Group: Allows hosts to transfer data in a common network configuration. These hosts must be explicitly involved in the networking activity, such as making routing decisions, for a protocol to be placed in this group.

(A) Network level, containing network-specific protocols that allow for data transfers over a single network of which the host is an integral part (i.e., host is also a network node).

(5) Subnet Protocol Group: These protocols are the lowest level protocols and are dependent on the underlying technology. They include protocols for transferring data between two physically separated entities, protocols with the ability to interface a host to a subnet, and protocols with the ability to access a shared communication media.

(A) Data link level, containing protocols that manage the transfer of data across a single data link.

(B) Physical level, containing protocols that provide mechanical, electrical, functional, and procedural requirements to access and to transfer data onto a physical communications channel. Often the physical level is embodied directly in hardware as opposed to software.

(C) Subnet level, containing protocols that interface a host computer or network front-end to a particular subnet.

(D) Access level, containing protocols which mediate access to a shared communications medium, such as coaxial cable or a free-space radio frequency channel.

4. DOD STANDARD PROTOCOLS.

A. Within the framework of the DoD reference model there are currently:

(1) Five DoD standard protocols (refs L-P) which are mandatory for use in all DoD packet switching networks to support their respective services.

(2) Two DDN/ARPANET access (host-to-IMP) protocols (refs R & S).

(3) Several evolving standards: User Datagram Protocol (UDP), Stream Protocol (STP), Gateway-to-Gateway Protocol (GGP), and Exterior Gateway Protocol (EGP). To provide the full range of services required, additional protocols will be needed and development will continue.

B. MIL-STD-1777, Internet Protocol (IP).

(1) IP is the underlying basis of the DoD internetwork architecture. It is to be provided in all DoD systems (refs A-E). It provides:

(A) Basic datagram service. (NOTE: A datagram is a packet of information which is treated independently of any other datagrams for the purposes of routing and delivery. Each datagram carries all information necessary to reach its destination.)

(B) Basis for dynamic and adaptive routing to compensate for network damage and congestion.

(C) Datagram fragmentation and ordered reassembly (matches networks whose datagram length is different).

(D) Internet addressing which uniquely identifies destination network, host and upper layer protocol. This service is critical in an internetwork environment where subnet addressing (e.g., within a local area network) is generally separately administrated.

(E) Security options (fields for security and compartment labels, handling restrictions, transmission control code, and loose and strict source and record route) and header checksum. (NOTE: IP is closely associated with ongoing efforts to develop and field end-to-end encryption through the internet private line interface (IPLI) and BLACKER programs.)

(F) Precedence. The IP "type of service" allows designation of precedence and trade-off between delay, reliability, and throughput. This provides a means of influencing the allocation of subnetwork resources and routing decisions.

(G) Mechanism for error reports and other control messages (separately specified Internet Control Message Protocol--ICMP).

(2) Applicability. "The Internet Protocol (IP) and the Transmission Control Protocol (TCP) are mandatory for use in all DoD packet switching networks which connect or have the potential for connecting across network or subnetwork boundaries. Network elements (hosts, front-ends, bus interface units, gateways, etc.) within such networks which are to be used for internetting shall implement TCP/IP. The term network as used herein includes local area networks (LANs) but not integrated weapon systems. Use of TCP/IP within LANs is strongly encouraged particularly where a need is perceived for equipment interchangeability or network survivability. Use of TCP/IP in weapon systems is also encouraged where such usage does not diminish network performance (ref L). The Air Force policy on protocols for packet-oriented LANs (reiterated and affirmed here) clarified this statement of applicability by designating TCP/IP as Air Force standards for connection-based transport and internet services within packet-oriented LANs (ref F). Due to the critical importance of inter-operability to achieve robust (flexible, survivable, and enduring) support for essential mission requirements, deviations to this policy require prior Air Staff approval (through MAJCOM/SOA channels to AF/SITT). Actions should be initiated to adapt existing systems to comply with this policy if (a) they interconnect or are planned for connection with other systems, or (b) they are reconfigured or modified to support additional functions or users.

C. MIL-STD-1778, Transmission Control Protocol.

(1) TCP was designed to operate above IP to provide reliable communications between pairs of processes in logically distinct hosts on a network or sets of interconnected networks. TCP serves as the basis for DoD-wide interprocess communication. TCP will operate successfully in an environment where the loss, damage, duplication, or misordering of data and network congestion

can occur. This robustness in spite of unreliable communications media makes TCP well-suited to adaptively support military requirements during stress. TCP provides connection-oriented (virtual circuit) data transfer which is reliable, ordered, full duplex and flow controlled. TCP includes the following mechanisms:

(A) PAR mechanism. Positive acknowledgement with retransmission is used with sequence numbers and checksums to support data reliability, integrity and security.

(B) Flow control mechanism. The receiving TCP can control the sending TCP's flow to preclude overflowing the receiver's buffers. This protects both the sending TCP from excessive retransmissions and, indirectly, precludes waste of resources of connecting networks.

(C) Multiplexing mechanism. TCP provides for multiple upper layer protocols within a single host and multiple processes in an upper layer protocol to use TCP simultaneously. This enables a single network connection for a host to simultaneously support multiple services/users.

(D) Security and precedence labelling. The security and precedence parameters are those used in IP and extend control closer to the end-user. In some applications, the TCP port may also be involved with access control.

(2) In order to obtain the full benefits of the connection-based reliable end-to-end services of TCP (to include flow control), the TCP implementation should be as close to the application process as possible, e.g., in the host. However, the need to reduce loading on the host (for example, with a microprocessor-based workstation) may require use of a front-end device to offload as many of the communications functions as possible. In these instances, care should be taken to maintain the range of services and flexibility associated with TCP. There are three primary methods of interfacing a host to a front-end implementation of TCP:

(A) The network handler in the host operating system may pass TCP commands and arguments to the front-end device. The front-end device passes the TCP commands and arguments to the TCP module. This provides minimal overhead in the host and maintains full TCP services. However, the host/front-end interface within both the host and front-end device is unspecified and does not support a general application. Consequently, a standard host-to-frontend protocol (HFP) is desired. An example of an HFP is the WWMCCS HFP developed for DCA (ref U). This HFP is also used for the DIA DODIIS network front-end. Pending development of an international/commercial standard HFP, the WWMCCS HFP should be used to the maximum extent feasible.

(B) Host operating system is not made "aware" of TCP and an exiting host protocol such as a terminal handler or disk controller is used. In this terminal or disk emulation mode, only a degenerate TCP service can be established. This defeats many of the TCP services. Further, required services will have to be established by ad hoc protocols (noninteroperable) established over the degenerated TCP connection. This approach should be avoided for other than interim implementations pending upgrade.

(C) "Front-end" can be displaced over a network into a gateway device. This has several serious problems. First, no matter how reliable the network is normally, its characteristics are subject to change (perhaps drastically), particularly under stress. Consequently, displacement of the end-to-end services away from the applications processes significantly increases the susceptibility of the transport mechanism to degradation, particularly relative to flow control. Second, the displacement of the reliable transport services to a gateway severely limits the survivability of this function even if the gateway function is provided redundancy. Without the gateway function, the host generally cannot operate in the internet environment even if a contingency/restoral circuit connects to another network. This is particularly critical to hosts requiring mobility or reutilization. Third, under this scheme there is no standardized, reliable transport mechanism available internal to the network for host-to-host interprocess communications. Such services are critical for file transfers, electronic mail, and other higher level services. Consequently, this approach should also be avoided.

(3) Applicability. The statement of application for TCP and Air Force policy on use of TCP within packet-oriented LANs is as specified above (para 4.B.(2)) for IP.

D. MIL-STD-1780, File Transfer Protocol (FTP). Though usable directly by a user at a terminal or workstation, FTP is designed mainly for use by programs.

(1) The objectives of FTP are as follows:

(A) To promote sharing of files (computer programs and/or data).

(B) To encourage indirect or implicit (via programs) use of remote computers.

(C) To shield a user from variations in file storage systems among hosts.

(D) To transfer data reliably and efficiently for use by programs.

(2) Applicability. "The file transfer protocol is mandatory for use in all DoD packet switching networks which connect or have the potential for utilizing connectivity across network and subnetwork boundaries and which require a file transfer service. The term network as used herein includes local area networks" (ref N).

E. MIL-STD-1781, Simple Mail Transfer Protocol (SMTP).

(1) Objectives. SMTP provides for the reliable and efficient transfer of electronic mail; directly from the sending user's host to the receiving user's host when the two hosts are connected to the same transport service, or via one or more relay SMTP-servers when the source and destination hosts are not connected to the same transport service.

(2) Applicability. "The simple mail transfer protocol is mandatory for use in all DoD packet switching networks which connect or have the potential for utilizing connectivity across network and subnetwork boundaries and which require a mail transfer service. The term network as used herein includes local area networks" (ref O).

F. MIL-STD-1782, TELNET Protocol.

(1) Objectives. TELNET provides a standard method of interfacing terminal devices and terminal-oriented processes to each other. The protocol may also be used for terminal-terminal communication (linking) and process-process communication (distributed computation).

(2) Applicability. "TELNET protocol is mandatory for use in all DoD packet switching networks which connect or have the potential for utilizing connectivity across network and subnetwork boundaries and which require a virtual terminal service. The term network network as used herein includes local area networks" (ref P).

G. FTP and similar higher level protocols are intended to insulate the end-users or end-users' programs by providing virtualized (logical) resources (for example, FTP partially implements the concept of a network virtual file system). These virtualized resources are implemented with a common intermediate representation (a notional resource) which builds services on defined primitive functions. To provide fully interoperable services, it is necessary that the notional or virtual resource be functionally limited to the set of services which can be supported by all actual resources (lowest common denominator). In order to provide enhanced services while still maintaining interoperability, the concept of negotiated service extension (options) is used. Either party (or both) may initiate a request that an option take effect. The other party may then either accept or reject the request based on its capabilities. This allows two communicating entities to raise the current level of service up to their highest common level. However, improper use of service extensions limits the number of compatible resources available. Unless programs are designed to continue to function (perhaps with some degradation or loss of efficiency) without these service extensions being available, their use will limit the degree of flexibility and survivability attainable.

H. DDN Access Protocols.

(1) The DDN is a packet switched network designed to fulfill DoD common-user data communications requirements (ref V).

(2) DDN evolved from the ARPANET and used the existing host interface protocol (1822 protocol, ref Q). However, commercial public data networks were implementing the international (CCITT) X.25 interface standard. Due to interoperability problems between different X.25 implementations, USDRE prohibited (ref D) the use of X.25 connections to the DDN until the DDN X.25 specification had been approved by the protocol standards steering group (PSSG). This approval was obtained and resulted in publication of the DDN X.25 specification (ref R). By ref E, USDRE authorized use of the DDN X.25 specification and directed that DDN X.25 become the primary DDN protocol. While the 1822 protocol will continue to be supported by the

DDN until phased out via evolution, it is DoD policy that all new systems and systems undergoing major redesign use levels 2 (link) and 3 (network/packet) of the DDN standard X.25 protocol for interfacing to the DDN. Exceptions to this policy require case-by-case waivers by ASD(C3I) (processed through command channels to AF/SITI).

(3) The DDN currently supports DDN basic X.25 service. At this level of service, X.25-connected hosts cannot interoperate with 1822-connected hosts. This is particularly critical to terminals connected to the DDN using DDN terminal access controllers (TACs). DDN TACs use 1822-connections and cannot interoperate with X.25-connected hosts. Development of DDN standard X.25 service is progressing and should be available by the 1st quarter FY86. DDN standard X.25 service will support interoperation between X.25-connected and 1822-connected hosts.

(4) Irrespective of the access protocol used (X.25 or 1822), interoperability between like-connected hosts, or eventually any hosts, requires the hosts (to include network front-ends) to implement the DoD standard higher level protocols (i.e., IP, TCP, FTP, SMTP and TELNET).

5. Due to the critical importance of interoperability and standard data communications protocols to achieving flexible and adaptive information systems capable of sustaining mission essential services under stress, the policies and guidelines contained herein will be included in the Air Force Information System Architecture and, as appropriate, its subordinate elements.

APPENDIX C

SUMMARY OF AFLANSPO USER REQUIREMENTS SURVEY

AS BRIEFED MARCH 1985

Requirements Survey Of Potential LAN Users Was Conducted

A survey was conducted of over 330 organizations involved in various aspects of information processing in the Air Force in the United States and abroad. Well over half of the surveyed organizations responded.

The survey dealt with the following areas:

Applications which need data communications

Number of devices to be networked now and in future

Mobility of devices

Connectivity among different types of devices

Access to long haul networks

Security

Survivability

Variety Of Applications Need Communications

The survey revealed that user organizations either have or are planning for a wide variety of applications which need communications. For example, electronic mail is an application which uses computers as post offices for electronic letters. This application requires communications to allow other computers to access the post office.

Survey Reveals The Need For Network Expandability And Device Mobility

The survey showed that the average number of devices that will be serviced by a single network on an Air Force base increases rapidly every year. The current number of devices serviced by a LAN is over 170, but within the next five years this number will reach over 1000.

Offices and personnel on Air Force bases move often. The networking scheme must handle this periodic relocation of devices as well as the rapid growth in the number of devices that must be networked.

Users Need Connectivity Between A Variety Of Devices And With Devices Outside The "Local Area"

Connectivity is the ability to communicate with other devices. Users need connectivity between a variety of devices such as terminal-to-host, host-to-host and workstation-to-workstation. Also, there is a need for connectivity between devices from different vendors. Devices in one local area need to communicate with devices on long haul networks.

Security And Survivability Are Growing Concerns

The average respondent to the survey reported that only 18% of their organization's information is classified. This is expected to increase to 28% within the next five years. The survey also indicated that 86% of all Air Force organizations will have a requirement for handling classified data.

The survey revealed that a significant percentage of Air Force local area networks will support command and control, and combat operations, or be exposed to combat operations or other damages. This requires the LAN to be survivable.

APPENDIX D

SAMPLE QUESTIONNAIRES FOR INTERCONNECTION SCENARIOS

SMALL ORGANIZATION

1. Point of Contact: Ms Pam Slotnik, (617) 555-1976

2. Organization and Mission: 11AF/JA, Hanscom AFB, MA 00111; base legal office. Our purpose in networking our devices is to facilitate transfer of information between computers in the office and to tie into the base electronic mail service and the Defense Data Network. A long term goal is to access other law libraries through public networks.

3. Organizational Structure:

Division Chief
Administration (1)

Research/Contracts Branch (4)   Legal Assistance Branch (4)

4. Physical Location: Bldg 74, rooms 1, 2, and 4

5. Existing Computer Locations:

Make/model (quantity)	Room #
Zenith 248	1
Zenith 150	1
IBM PC	2
Zenith 100 (3)	2
IBM PC	4
Zenith 100 (2)	4
Zenith 150	4

6. How often the equipment will be moved: The office has no plans to relocate in the foreseeable future. Equipment will not move when personnel relocate for permanent change of station or temporary duty.

7. Security: Currently there are no security requirements for this office, however, there are significant privacy act constraints.

8. Survivability/Reliability: No survivability requirement exists. A 90% reliability during office hours; normal office hours are 0700-1730, M-F.

9. Installation Considerations: If possible, installation should occur outside normal office hours.

10. Systems and Services (list host operating systems, software supported, peripherals, etc): All PCs use MS/DOS 2.11. The following programs are used: WORDSTAR, SIDEKICK, LOTUS 1-2-3, and BITCOM. There is one HP LASERJET and three EPSON FX printers. There is a 50Mbyte hard disk in the Z-248. Using a modem, the communications software, and emulating a terminal, the PCs can access the Harvard Law School legal database for research and case references.

LARGE, GEOGRAPHICALLY CONCENTRATED ORGANIZATION

1. Point of Contact: Capt Joe Smith, (618) 555-1234

2. Organization and Mission: HQ AFCC, Scott AFB, IL 62224; sets communications policy for the United States Air Force. Our goal is to connect the headquarters with a network enabling rapid transfer of information between deputates and within deputates. This network will not only support internal traffic but will also support electronic mail with the rest of the base and over the DDN. We want to become a showcase for networks for the Air Force.

3. Organizational Structure: see attached organizational chart.

4. Physical Location: Bldg 70.

5. Existing Computer Locations: There are 250 PCs and four mainframes. There are 75 PCs on the first floor, 100 on the second, and 75 on the third. The mainframes are located in a special equipment room in the basement. Capt Smith has a list of all computers by serial number and location.

6. How often the equipment will be moved: There is usually some movement of personnel and directorates each year. About 25 people are involved in these relocations. Our long term goal is to add 250 PCs so every member of the headquarters has one on his desk.

7. Security: We would like to evolve to a multilevel secure network as soon as the DDN can support secure traffic.

8. Survivability/Reliability: The mainframes are in a hardened environment, but the rest of the building is not built to survive a direct attack (conventional or nuclear); ensure the wiring scheme protects the mainframes from EMP effects. The system should operate with 95% reliabilty between the hours of 06001830, M-F, and 0800-1300, Sat.

9. Installation Considerations: Installation should occur in only one section of the building at a time. Installation in the command section and the DCS offices should occur at night.

10. Systems and Services (list host operating systems, software supported, peripherals, etc): Most PCs use MS/DOS 3.0; some use CPM. The following programs are used: WORDSTAR, SIDEKICK, LOTUS 1-2-3, PEACHTEXT, PEACHCALC, MS WORD, KERMIT, ACCESS. There are many types of printers at the headquarters (about 200). At least 75 printers are letter quality. There are also two HP plotters used for making overhead view-graphs. The mainframes are VAX 11/780s and use the DEC operating system.

LARGE, GEOGRAPHICALLY DISPERSED ORGANIZATION

1. Point of Contact: Capt Sally Jones, (202) 555-7890

2. Organization and Mission: 93rd Test and Evaluation Squadron, Bolling AFB, MD 21333; our squadron designs, and tests computer chips for DoD. We recommend policy to the Defense Communications Agency and evaluate recommendations made by other services and organizations. We also write technical manuals and test procedures for applications designed here and at Wright-Patterson AFB. We require a secure network to support this mission.

3. Organizational Structure: see attached organizational chart.

4. Physical Location: Bldgs 290-295, 14, 100, 110, and 112.

5. Existing Computer Locations: See attached map and list.

6. How often the equipment will be moved: Due to the secure nature of some of the work, movement is kept to a minimum and should not be part of the planning process.

7. Security: We have a requirement for a multilevel secure network as soon as possible.

8. Survivability/Reliability: Each building should be capable of operating its portion of the network alone. The network should be resistant to EMP effects. A reliability of 90% for the entire network and 95% for each building is required.

9. Installation Considerations: Installation should occur in only one building at a time. Installation should outside normal duty hours (0715-1630, M-F), if possible. Escorts will be required for installation in bldgs 14 and 292.

10. Systems and Services (list host operating systems, software supported, peripherals, etc): Most PCs use MS/DOS 3.0; some use CPM. The following programs are used: WORDSTAR, MACPAINT, BORLAND'S CAD/CAE, MS WORD. There are many types of printers and plotters. Currently most are dedicated to a particular workstation/PC.

LIST OF REFERENCES

1. 1842 EEG survey, "EIFEL Networking Requirements at Spangdahlem AB," September 1983.

2. Booz-Allen & Hamilton, System Specification for the Air Force Unified Local Area Network Architecture (Type A), Spec No OCC-2-283, 10 October 1983.

3. Chorafas, Dimitris N., Designing and Implementing Local Area Networks, McGraw-Hill, Inc., New York, NY, 1984.

BIBLIOGRAPHY

Anon., "Introduction to Packet Switching Technology," pamphlet, no date.

Ballenger, Wesley A. Jr., Thesis, "Modeling Security in Local Area Networks," Air Force Institute of Technology, December 1983.

Bartee, T.C. and O.P. Buneman, "C3I Local Area Networks--An Assessment," IDA Paper P-1715, Institute for Defense Analyses, June 1983.

Black, Uyless D., Data Communications, Networks and Distributed Processing, Reston Publishing Company, Inc., Reston, VA, 1983.

Chorafas, Dimitris N., Designing and Implementing Local Area Networks. , McGraw-Hill, Inc., New York, NY, 1984.

Datapro, All About Local Area Networks and PABX Systems, McGraw-Hill, Inc., New York, NY, 1984.

Datapro, Local Area Networks and the Data Communications Capabilities of PABXs, McGraw-Hill, Inc., New York, NY, 1985.

Foster, Frederick J., "The Feasibility of Local Area Information Networks for US Air Force Aircraft Operations Support," Air Command and Staff College Report # 83-0750, 1983.

Jacobs, Charles E. and David M. Norman, Research Report, "Data Network Management: Options and Opportunities," Air Force Communications Command, December 1983.

Ritter, Richard A., "A Generic Model for a Base Level Information Transfer Network," Air Command and Staff College Report # 84-2175, 1984.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Superintendent Attn: Prof Neil Rowe, Code 52RP Naval Postgraduate School Monterey, California 93943-5002	1
4.	JDSSC/C333 Attn: Capt Jannine C. Mathis Pentagon Washington, DC 20301-7010	1
5.	Superintendent C3 Academic Group Naval Postgraduate School Monterey, California 93943-5000	1

Thesis
C5097 Cleveland
c.1 A methodology for designing local area networks for the Air Force.